

# **An Experiment with CC Version 3.0 Migration**

## **Abstract:**

A draft EAL4 (with augmentation) protection profile (sans rationale sections) has been developed for a multilevel print server (MPS). A MPS must enforce a mandatory access control policy regarding input received from networks at different sensitivity levels, and must provide trusted separation pages indicating the sensitivity level of print jobs sent to a system high printer. The MPS also enforces supporting policies and services to include: detection of malicious print jobs, audit (generation, logging and alarms), identification and authentication, administrative tools, and operator services.

The MPS TOE consists of two components: an underlying high assurance separation kernel (SK) and an MPS “application”. The composed nature of the TOE, building on an evaluated separation kernel, represents a challenge with respect to the allocation of mandatory policy and supporting policies between elements of the MPS application and the SK.

The MPS protection profile (MPS PP) draft was written using the Common Criteria (CC) Version 2.2. It included security functional requirements derived from the following classes: FAU, FCS, FDP, FIA, FMT, FPT, FRU, FTA and FTP. Since the MPS system is intended to be used in environments requiring medium robustness, the targeted evaluation level is EAL4+ (i.e., EAL4 augmented with flaw remediation and maintenance of assurance components.) Although most of the security assurance requirements in the MPS PP were selected from the base set of EAL4 requirements without modifications, some requirements in the ADV and AGD classes were modified (and made explicit) to satisfy MPS-specific security objectives.

In CC Version 3.0, many of the functional and assurance requirements used in the MPS PP have been drastically modified and in some cases removed entirely. Composition issues were also addressed in v3.0 in the form of the new ACO class. At our institution, a new course on security requirements derivation using the CC framework was recently introduced into the Computer Science curriculum. To provide a faculty exercise in understanding CC v3.0, the MPS PP draft was migrated to CC v3.0. With the knowledge that CC v3.0 is being revised, this activity contributed to our ongoing effort to be current with the latest CC developments.

This paper presents our experience in working with the new approaches to both functional and assurance requirements in CC v3.0. It also discusses transitional issues in areas that were significantly changed in CC v3.0 such as the mapping of the security management functions in v2.2 [FMT] into different components in CC v3.0 [e.g., FDP\_ACC, FDP\_MSA].